Kemp Web Application Firewall

Feature Description

UPDATED: 27 April 2021

Copyright Notices

Table of Contents

1 Introduction 5

1.1 Document Purpose 6

1.2 Intended Audience 6

1.3 Related Firmware Version 6

2 Configuring WAF 7

2.1 Resource Considerations 7

2.2 Balancing WAF Resource Utilization with High Load Applications 7

2.3 Managing Daily Updates 8

2.3.1 Automatic Downloading and Updating of Daily Updates 8

2.3.2 Manual Downloading and Updating of Daily Updates 10

2.4 Custom Rules 11

2.4.1 Delete/Download a Custom Rule or Data File 12

2.5 Configure WAF for a Virtual Service 12

2.5.1 Advanced Settings 14

2.5.2 False Positive Analysis 16

2.6 Backing Up and Restoring a WAF Configuration 18

2.7 WAF Logging, Statistics and Status Options 18

2.7.1 Export Logs in the Web Application Firewall menu 19

2.7.2 WAF Event Log 20

2.7.3 WAF Options in the Extended Log Files Screen 20

2.7.4 Enable WAF Debug Logging 22

2.7.5 WAF Statistics 23
2.7.5.1 Home Page 23
2.7.5.2 Statistics Page 23
2.7.6 WAF Misconfigured Virtual Service Status 24
3 Troubleshooting 25
3.1 WAF Logging 25
3.2 WAF Compatibility with Kerberos Constrained Delegation (KCD) 25
3.3 Unable to Download/Update Daily Updates 25
Appendix A: Legacy Rules 27
Configure WAF Options (Legacy) for a Virtual Service 27
WAF Options (Legacy) in the Virtual Service Modify Screen 29
References 34
Last Updated Date 35

1 Introduction

With cybercriminal attacks on the rise, organizations need to do more than ever to mitigate risks to their applications on the web. Application security is a multifaceted and ever-changing task and must be applied at multiple levels of the infrastructure that serves applications. Security must be provided on the network before requests reach the backend application servers, and Kemp has the experience and the tools you need to do this. Deploying LoadMaster with the Kemp Web Application Firewall (WAF) enabled as part of your network infrastructure helps deliver in-depth security for your web servers and applications.

The Kemp Web Application Firewall (WAF) enables secure deployment of web applications, preventing Layer 7 attacks while maintaining core load balancing services, ensuring comprehensive application delivery and security. WAF functionality directly augments the LoadMaster’s existing security features to create a layered defense for web applications - enabling a safe, compliant and productive use of published services.

> WAF is only available on certain subscriptions. Please contact a Kemp representative if needed.

When WAF is enabled, the WAF engine scans every incoming HTTP packet – running through each assigned rule individually and deciding what action to take if a rule is triggered. The rules can be run on requests and responses.

WAF can protect against attacks, such as:

- SQL Injection
- Cross-Site Scripting (XSS)
- Unvalidated redirects and forwards
- Missing function-level access control
- Sensitive data exposure
- Security misconfiguration
- Broken authentication and session management

For a more detailed overview of the WAF feature, refer to the WAF section in the **Kemp LoadMaster, Product Overview**.

1.1 Document Purpose

The purpose of this document is to describe the WAF features and provide step-by-step instructions on how to configure the WAF settings in the Kemp LoadMaster.

For further information and assistance, refer to our Kemp Support site for Support contact details: http://kemptechnologies.com/load-balancing-support/kemp-support/.

1.2 Intended Audience

This document is intended to be read by anyone interested in finding out more about the Kemp WAF functionality.

1.3 Related Firmware Version

This document was published with LoadMaster Operating System (LMOS) version 7.2.54. This document has not required substantial changes since 7.2.54. However, the content is in sync with the latest LoadMaster Generally Available (GA) firmware.

2 Configuring WAF

2.1 Resource Considerations

> Utilizing WAF can have a significant performance impact on the LoadMaster deployment. Please ensure that the appropriate resources are allocated.

For virtual and bare metal LoadMaster instances, a minimum of 2GB of allocated RAM is required for the operation of WAF. The default memory allocation for Virtual LoadMasters and LoadMaster Bare Metal instances before LoadMaster Operating System version 7.1-22 is 1 GB of RAM. If this default allocation has not been changed, modify the memory settings before proceeding with the WAF configuration. If the check box to enable WAF is grayed out, it could mean that the LoadMaster does not have enough memory to run WAF.

There is a WAF engine open connection limit of 64000 per Virtual Service.

2.2 Balancing WAF Resource Utilization with High Load Applications

The WAF subsystem uses a significant amount of system resources. When enabling WAF, you should avoid overconsuming system resources that are needed for load balancing Virtual Services. When WAF starts to consume resources at a level that impacts overall system performance, one or more of these symptoms can be observed:

- High CPU utilization
- High memory utilization
- InterProcess Communication (IPC) issues between Layer 7 and WAF processes
- Decreased Virtual Service throughput
- Increased Virtual Service latency

There are essentially two ways of dealing with these issues:

- Disable WAF completely on one or more Virtual Services.

- Tailor the applied rulesets used on each Virtual Service to reduce the rules applied to the minimum necessary for secure operation.

The best practice for WAF rulesets is to avoid a blanket application of a ruleset and instead, enable only those rules in the ruleset that are specifically required for your application.

Note that internal processing and communication between WAF and Layer 7 in version 7.2.36 is enhanced to help mitigate resource exhausting issues through smarter thread and resource management. The best practice is still to enable a minimum set of rules instead of enabling the entire ruleset.

2.3 Managing Daily Updates

The Kemp-provided daily updates can be set to download automatically and install. They can also be manually downloaded and installed. The sections below explain how to use each method.

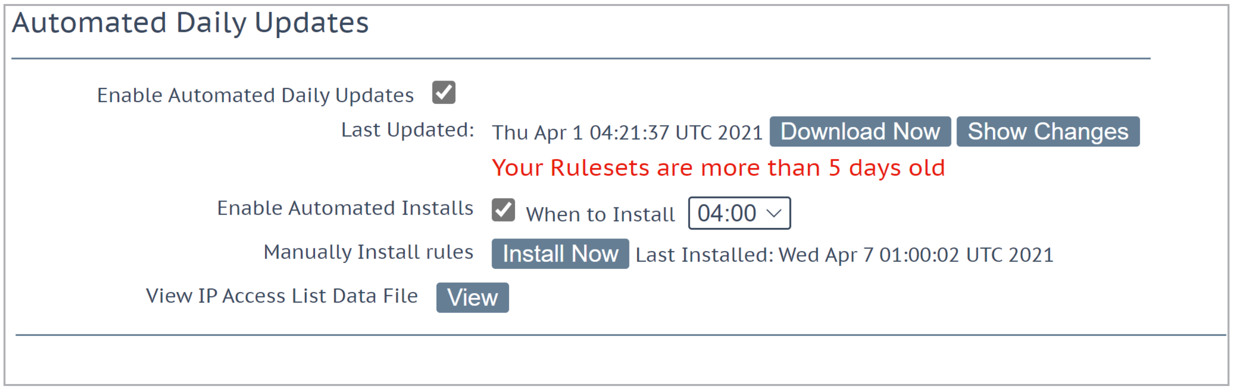
The IP/FQDN and port of the Kemp licensing server must be open on your firewall. The FQDN and IP address is **licensing.kemp.ax 52.166.52.190**, and the port is **443**. The old FQDNs for the Kemp licensing server are **alsi.kemptechnologies.com** and **alsi2.kemptechnologies.com**, and the IP address for the old FQDNs is **52.136.251.129**. These also may need to be open depending on your LoadMaster version.

Kemp-provided daily updates are only available when you have an Enterprise Plus subscription. For further details on the subscription tiers, go to LoadMaster Support Subscriptions.

2.3.1 Automatic Downloading and Updating of Daily Updates

Before enabling the automatic installation ofdaily updates, you must first download and install the latest updates. Follow the steps below to configure automatic download and installation settings for latest updates:

1. In the main menu, select **Web Application Firewall > Access Settings**.



Automated Daily Updates

Enable Automated Daily Updates ☑

Last Updated: Thu Apr 1 04:21:37 UTC 2021

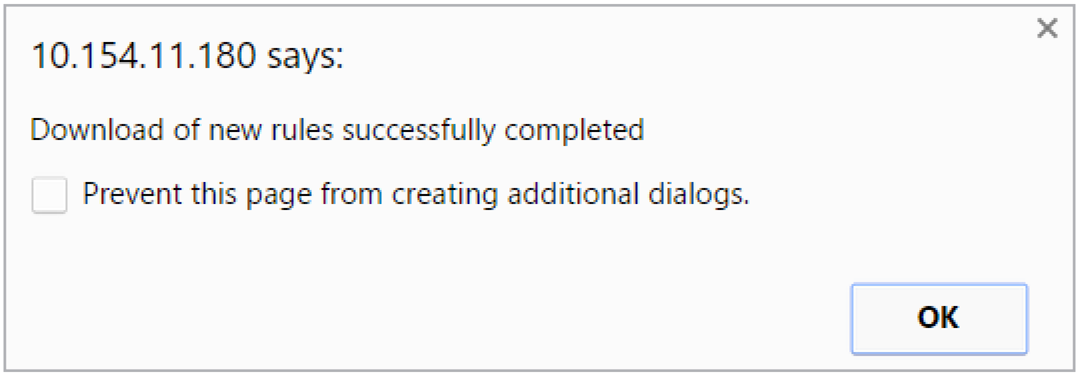
Your Rulesets are more than 5 days old

Enable Automated Installs ☑ When to Install 04:00

Manually Install rules — Last Installed: Wed Apr 7 01:00:02 UTC 2021

View IP Access List Data File

2. Click the **Download Now** button to download the latest daily updates.



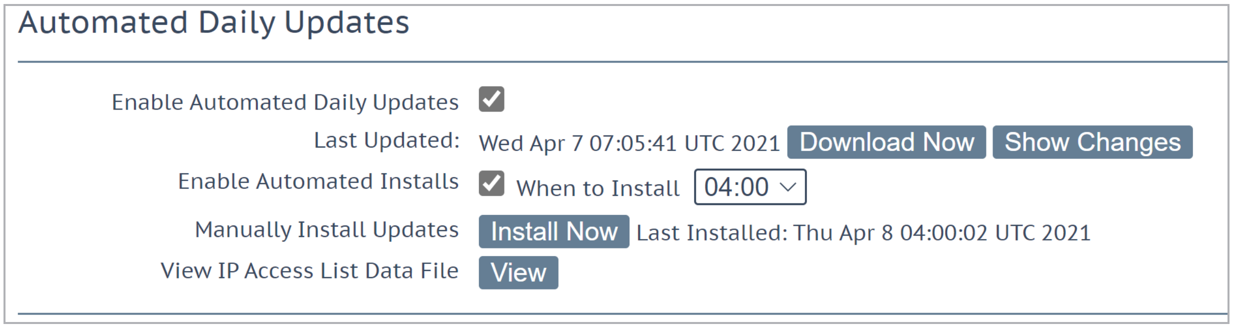
10.154.11.180 says:

Download of new rules successfully completed

□ Prevent this page from creating additional dialogs.

3. Click **OK** on the success message.

4. Click **Install Now** to install the latest daily updates.



Automated Daily Updates

Enable Automated Daily Updates ☑

Last Updated: Wed Apr 7 07:05:41 UTC 2021

Enable Automated Installs ☑ When to Install 04:00

Manually Install Updates — Last Installed: Thu Apr 8 04:00:02 UTC 2021

View IP Access List Data File

5. To enable the automatic download of daily updates, select the **Enable Automated Daily Updates** check box.

The automatic and manual download options are grayed out if WAF support has expired. If this is the case, contact Kemp to renew your subscription.

6. To enable automatic installation of the daily updates, select the **Enable Automated Installs** check box.

By default, the **Enable Automated Installs** and **Manually Install Updates**options are grayed out. The rules must be downloaded for the first time before these options become available.

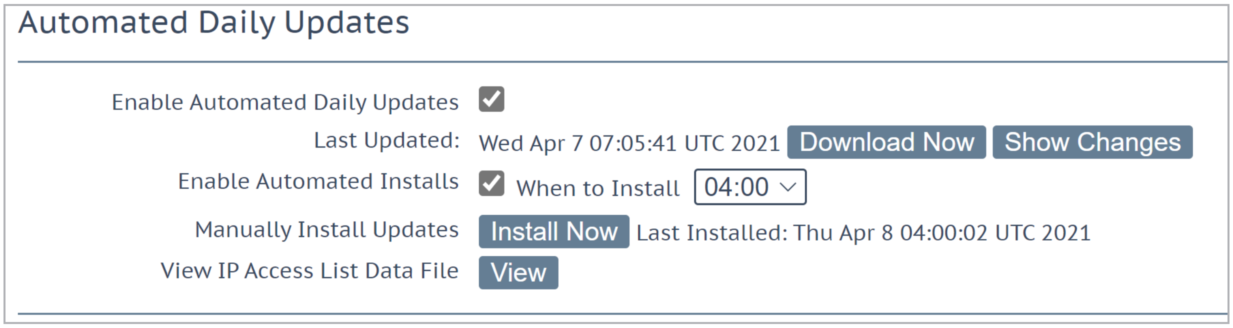
7. Select the time (hour of the day) to install the daily updates automatically.

The daily updates must be assigned to a Virtual Service to take effect.

2.3.2 Manual Downloading and Updating of Daily Updates

To manually download and install the daily updates, follow the steps below:

1. In the main menu, select **Web Application Firewall > Access Settings**.



Automated Daily Updates

Enable Automated Daily Updates ☑

Last Updated: Wed Apr 7 07:05:41 UTC 2021

Enable Automated Installs ☑ When to Install 04:00

Manually Install Updates Last Installed: Thu Apr 8 04:00:02 UTC 2021

View IP Access List Data File

2. Click **Download Now** to download the daily updates now.

A warning message appears if the rules have not been updated in the last seven days or if they have not been downloaded at all.

3. After the daily updates are downloaded, the **Show Changes** button appears. Click this button to retrieve a log of changes that have been made to the Kemp WAF rule set.

4. Click **Install Now** to install the daily updates manually.

The daily updates must be assigned to a Virtual Service in order to take effect.

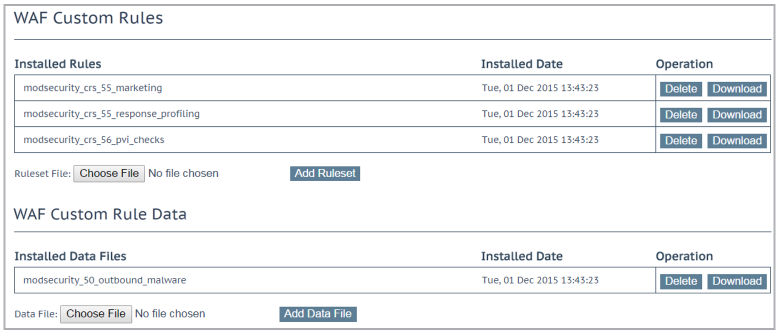
2.4 Custom Rules

Third-party rules can be uploaded to the LoadMaster. You can also write your own custom rules, which can be uploaded. These rules must be in the ModSecurity rule format in order to upload correctly. The **Custom Rules** screen enables you to upload **WAF Custom Rules** (.conf) and associated **WAF Custom Rule Data** (.data or .txt) files. You can also upload gzip-compressed Tarball files (.tar.gz), which contain multiple rule and data files.

> Kemp does not recommend using the WAF rule "redirect" action in custom rules because of the impact this has on system performance. You should use content rules instead for that purpose.

To upload rule and data files, follow the steps below:

1. In the main menu, select **Web Application Firewall > Custom Rules**.



WAF Custom Rules

Installed Rules	Installed Date	Operation
modsecurity_crs_55_marketing	Tue, 01 Dec 2015 13:43:23	Delete Download
modsecurity_crs_55_response_profiling	Tue, 01 Dec 2015 13:43:23	Delete Download
modsecurity_crs_56_pvi_checks	Tue, 01 Dec 2015 13:43:23	Delete Download

Ruleset File: Choose File No file chosen Add Ruleset

WAF Custom Rule Data

Installed Data Files	Installed Date	Operation
modsecurity_50_outbound_malware	Tue, 01 Dec 2015 13:43:23	Delete Download

Data File: Choose File No file chosen Add Data File

2. To upload custom rules; in the **Installed Rules** section, click **Choose File**.

   Individual rules can be uploaded as .conf files. Alternatively, you can load a package of rules in a .tar.gz file.

3. Browse to and select the rule file(s) to be uploaded.

4. Click **Add Ruleset**.

5. To upload any additional data files, in the **WAF Custom Rule Data** section, click **Choose File**.

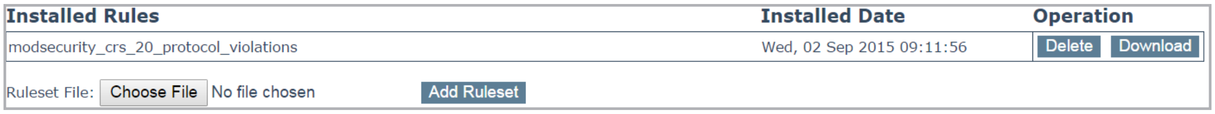
   The additional files are for the rules’ associated data files. If you uploaded a Tarball in the **Browse to and select the rule file(s) to be uploaded.** step, the rules and data files can be packaged together.

6. Browse to and select the additional data files to be uploaded.

7. Click **Add Data File**.

The rules are now available to assign within the Virtual Services modify screen. Refer to the next section to determine how to configure the Virtual Service to use the installed rules.

2.4.1 Delete/Download a Custom Rule or Data File



Installed Rules	Installed Date	Operation
modsecurity_crs_20_protocol_violations	Wed, 02 Sep 2015 09:11:56	Delete Download

Ruleset File: Choose File No file chosen

Custom rules and data files can be deleted or downloaded by clicking the relevant buttons.

> If a rule is assigned to a Virtual Service, it will not be available for deletion.

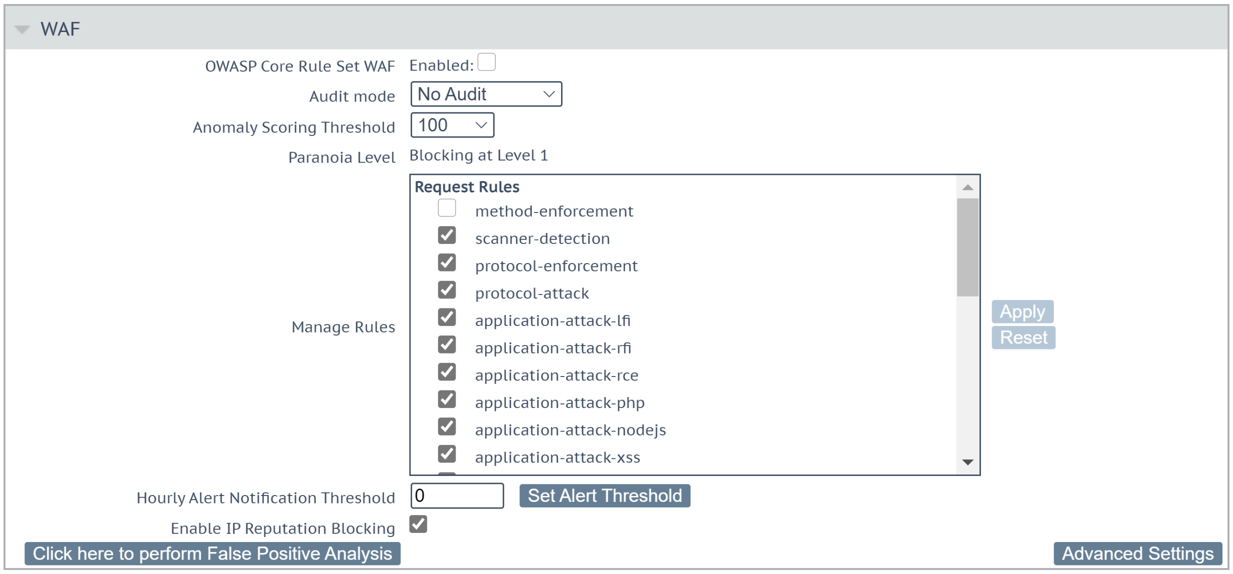
2.5 Configure WAF for a Virtual Service

WAF settings can be configured for each Virtual Service. Follow the steps below to configure the WAF in a Virtual Service. For more information on each of the fields, refer to the **<b>WAF UI Options</b>** section.

1. In the main menu of the LoadMaster UI, select **Virtual Services >View/Modify Services**.

2. Click **Modify** on the relevant Virtual Service.

3. Expand the **WAF** section.



WAF

OWASP Core Rule Set WAF Enabled: □

Audit mode: No Audit

Anomaly Scoring Threshold: 100

Paranoia Level: Blocking at Level 1

Manage Rules:

Request Rules
- □ method-enforcement
- ☑ scanner-detection
- ☑ protocol-enforcement
- ☑ protocol-attack
- ☑ application-attack-lfi
- ☑ application-attack-rfi
- ☑ application-attack-rce
- ☑ application-attack-php
- ☑ application-attack-nodejs
- ☑ application-attack-xss

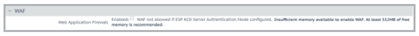
Hourly Alert Notification Threshold: 0

Enable IP Reputation Blocking: ☑

4. By default, WAF is disabled. To enable WAF, select **Enabled**.

When WAF is enabled for a Virtual Service, the section heading in the Virtual Service options changes from **WAF** to **WAF - Enabled**

The maximum number of WAF-enabled Virtual Services is the total (unused or available) RAM (in MB)/512 MB. For example: 8 GB/512 MB = 16 WAF-enabled Virtual Services. When the maximum is reached, no additional Virtual Services can be enabled with WAF.


WAF

Web Application Firewall Enabled: □ WAF not allowed if ESP KCD Server Authentication Mode configured. **Insufficient memory available to enable WAF. At least 512MB of free memory is recommended.**

A message displays if there is insufficient memory available to enable WAF.

A message is displayed next to the **Enabled** check box displaying how many WAF-enabled Virtual Services exist and the maximum number of WAF-enabled Virtual Services that can exist. If the maximum number of WAF-enabled Virtual Services is reached, the **Enabled** check box is grayed out.

5. Specify the **Audit mode**.

There are three audit modes:
- **No Audit:** No data is logged.
- **Audit Relevant:** Logs data that is of a warning level and higher. This is the default option for this setting.
- **Audit All:** Logs all data through the Virtual Service.

Selecting the **Audit All** option produces a large amount of log data. Kemp does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

6. Specify the **Anomaly Scoring Threshold**.

For each request, every triggered detection raises the anomaly score, most rules having a score of 5. If the cumulative anomaly score per request hits the configured limit, the request will be blocked. The default value is 100 and allowable range is 1 to 10000.

7. The Paranoia Level can be set in **Advanced Settings**, but the value is displayed here for informational purposes.

8. Enable or disable rules in the **Manage Rules** section. When finished making changes, click **Apply**.

Rules are grouped in the **Request Rules** section as per the OWASP numbering system. Rule groups or Individual rules within each ruleset can be enabled/disabled as required. To enable a rule or group of rules, select the relevant check box. If you have previously enabled/disabled rules in that ruleset, within that Virtual Service – the rules retain their previous settings.

Some rules or rule sets may have dependencies on other rules. There is no dependency check in the LoadMaster when rules are disabled - before disabling any rule, be aware of any rule chains or dependencies.

In the **Workloads** section there are several workloads available. When a workload is selected, the OWASP CRS optimizes the rules to ensure that known false positives are not returned.

If a user has created custom rules, they can be enabled or disabled within the **Custom Rules** section.

9. Specify the **Hourly Alert Notification Threshold** and click **Set Alert Threshold**.

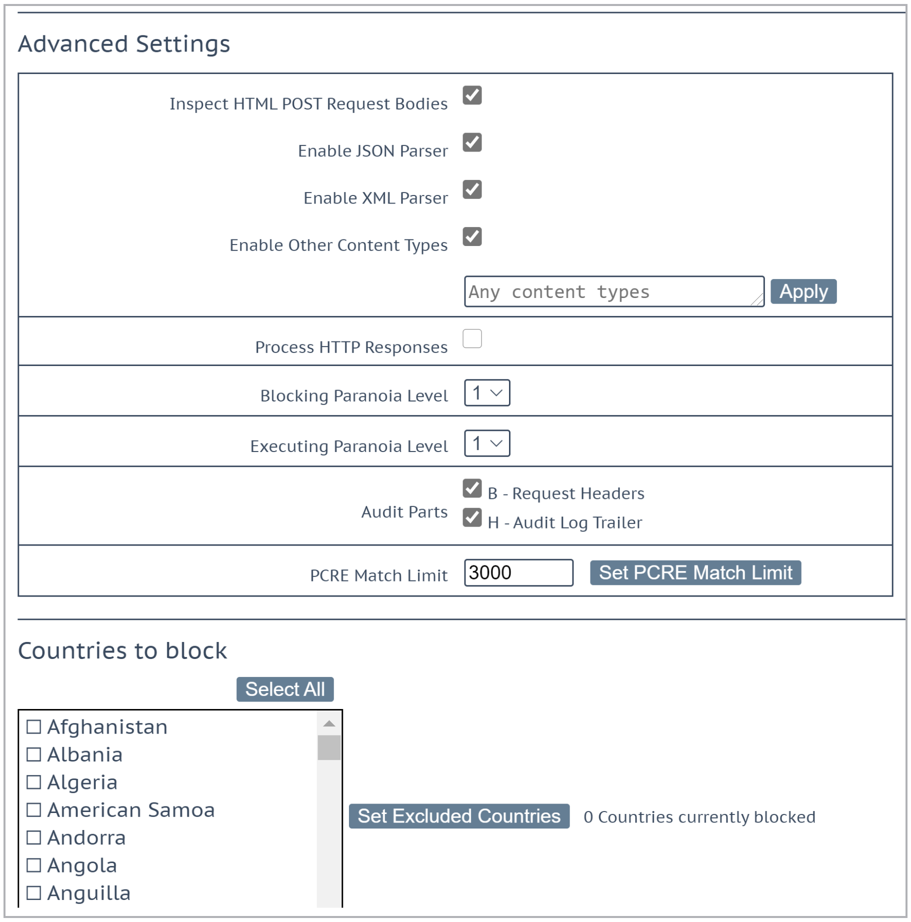
This is the number of incidents per hour before sending an alert. Setting this to **0** disables alerting.

10. To enable the **IP Reputation Blocking** rule set, select the **IP Reputation Blocking** check box.

This **IP Reputation Blocking** rule set enables the checking of client addresses against the IP reputation database.

2.5.1 Advanced Settings

Click the **Advanced Settings** button to configure the advanced OWASP settings.



Advanced Settings

Inspect HTML POST Request Bodies ☑

Enable JSON Parser ☑

Enable XML Parser ☑

Enable Other Content Types ☑

Any content types Apply

Process HTTP Responses ☐

Blocking Paranoia Level 1

Executing Paranoia Level 1

Audit Parts ☑ B - Request Headers ☑ H - Audit Log Trailer

PCRE Match Limit 3000 Set PCRE Match Limit

Countries to block

Select All

☐ Afghanistan
☐ Albania
☐ Algeria
☐ American Samoa
☐ Andorra
☐ Angola
☐ Anguilla

Set Excluded Countries 0 Countries currently blocked

1. Specify whether or not to Inspect **HTML POST Request Bodies**.

   The Inspect **HTML POST Request Bodies** option is disabled by default. If you enable this option, three more check boxes become available that allow you to enable the processing of JavaScript Object Notation (JSON), XML requests, and other content types.

2. Select **Process HTTP Responses** to enable checking of the responses from the server to the client.

   Enabling the **Process HTTP Responses** option makes two more options, **E - Intended Response Body** and **F- Response Headers**, available in the **Audit Parts** options

   The processing of response data can be CPU and memory intensive and may impact on performance.

3. Select the **Blocking Paranoia Level** to define how strictly the ModSecurity engine implements each rule.

The default Paranoia Level value is set at 1. With each paranoia level increase, the CRS enables stricter implementations of the rules, giving you a higher level of security. However, higher paranoia levels also increase the possibility of blocking some legitimate traffic due to false positives. If you use higher paranoia levels, you will likely need to add some exclusion rules for certain applications that need to receive complex input patterns.

4. Select the **Executing Paranoia Level** that defines the paranoia level at which the ModSecurity engine checks/verifies the requests coming from the servers. The results of the checks will be logged but the **Executing Paranoia Level** is not used to determine what traffic will be blocked.

   Though the **Executing Paranoia Level** can be higher than the **Blocking Paranoia Level**, it cannot be lower. A higher **Executing Paranoia Level** enables users to see which rules would be triggered at a higher Paranoia level without blocking traffic.

5. **Audit Parts:** A single string that contains the sections that are to be entered in the WAF audit log for each request. The supported values are A, B, E, F, H, K, Z,though only the values B, E, F, H can be enabled or disabled.

   For further information regarding the Audit Parts, please refer to https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-2-Data-Formats

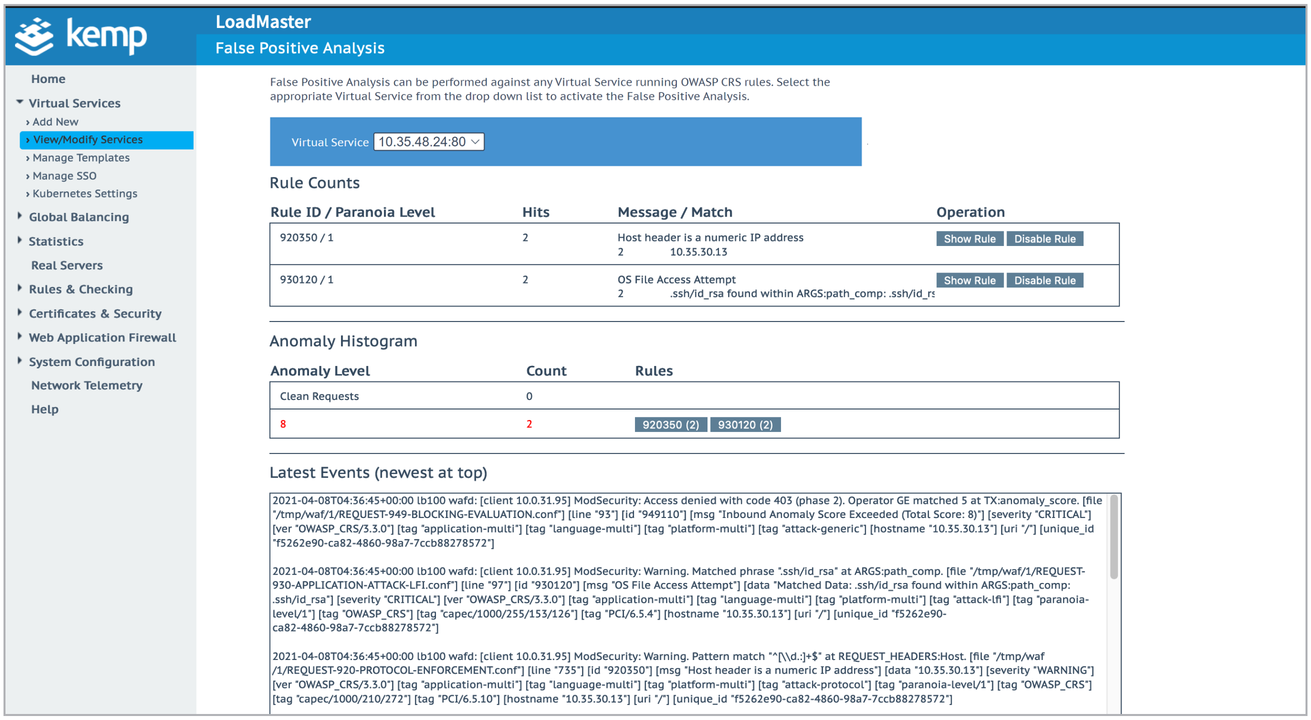
6. **PCRE Match Limit**: Set the PCRE Match Limit value and click the Set PCRE Match Limit button. The default value is 3000.

   This setting sets the maximum iterations that are internal PCRE engine will use before failing a match. Lower value may cause a valid match to fail, whereas a higher value may cause the WAF engine to run slower. This setting can be used to protect against Denial of Service attacks using complex regular expressions.

7. **Countries to block**: Based on GEO IP information, you can select countries that should not be allowed access. Click the **Select All** button to block the access for all countries or select individual countries from the country list that are to be blocked and click the **Set Excluded Countries** button.

2.5.2 False Positive Analysis

Click the **Click here to perform False Positive Analysis** button to check False Positives against any virtual service that runs OWASP CRS rules.



False Positive Analysis can be performed against any Virtual Service running OWASP CRS rules. Select the appropriate Virtual Service from the drop down list to activate the False Positive Analysis.

Virtual Service 10.35.48.24:80

Rule Counts

Rule ID / Paranoia Level	Hits	Message / Match	Operation
920350 / 1	2	Host header is a numeric IP address 2 10.35.30.13	Show Rule Disable Rule
930120 / 1	2	OS File Access Attempt 2 .ssh/id_rsa found within ARGS:path_comp: .ssh/id_rs	Show Rule Disable Rule

Anomaly Histogram

Anomaly Level	Count	Rules
Clean Requests	0	
8	2	920350 (2) 930120 (2)

Latest Events (newest at top)

```
2021-04-08T04:36:45+00:00 lb100 wafd: [client 10.0.31.95] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file "/tmp/waf/1/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 8)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "10.35.30.13"] [uri "/"] [unique_id "f5262e90-ca82-4860-98a7-7ccb88278572"]

2021-04-08T04:36:45+00:00 lb100 wafd: [client 10.0.31.95] ModSecurity: Warning. Matched phrase ".ssh/id_rsa" at ARGS:path_comp. [file "/tmp/waf/1/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "97"] [id "930120"] [msg "OS File Access Attempt"] [data "Matched Data: .ssh/id_rsa found within ARGS:path_comp: .ssh/id_rsa"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/255/153/126"] [tag "PCI/6.5.4"] [hostname "10.35.30.13"] [uri "/"] [unique_id "f5262e90-ca82-4860-98a7-7ccb88278572"]

2021-04-08T04:36:45+00:00 lb100 wafd: [client 10.0.31.95] ModSecurity: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/tmp/waf/1/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "735"] [id "920350"] [msg "Host header is a numeric IP address"] [data "10.35.30.13"] [severity "WARNING"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/210/272"] [tag "PCI/6.5.10"] [hostname "10.35.30.13"] [uri "/"] [unique_id "f5262e90-ca82-4860-98a7-7ccb88278572"]
```

Rule Counts

The Rule Counts section displays information on any rules that are being triggered by requests. Displays the Rule ID, the paranoia level the rule is running under, the number of hits per requests that have triggered the rule and the message or match for the request are displayed for each rule that is triggered.

Clicking the **Show Rule** button in the **Operation** column displays the contents of the rule file associated with the triggered rule. This opens in a separate tab and the URL contains the triggered rule id..

The rule can be disabled by clicking the **Disable Rule** button.

Anomaly Histogram

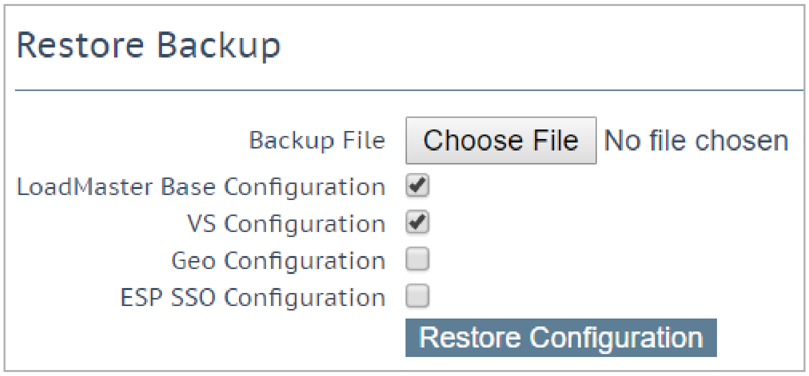
The first row of the **Anomaly Histogram** section displays how many requests have been run without triggering a rule.

Each subsequent row gives details of rules that have been triggered and which are affecting the Anomaly Score. In each row the cumulative Anomaly Score, the number of requests which have triggered the rule and the rule details are provided

Latest Events (newest at top)

Displays the event details for each rule that is triggered. These messages are in the standard ModSecurity log format and contains the anomaly score, the warning message, the attack state, and the paranoia level.

2.6 Backing Up and Restoring a WAF Configuration



Restore Backup

Backup File: Choose File No file chosen

LoadMaster Base Configuration ☑

VS Configuration ☑

Geo Configuration ☐

ESP SSO Configuration ☐

A backup of the LoadMaster configuration can be taken by going to **System Configuration > System Administration > Backup/Restore** and clicking **Create Backup File**.

The configuration can be restored from this screen also. Note that the Virtual Service settings can be restored by selecting **VS Configuration**, and the rules can be restored by selecting **LoadMaster Base Configuration**.

> The base configuration preserves the IP configuration information. The IP configuration information will need to be reconfigured when you restore the LoadMaster Base Configuration

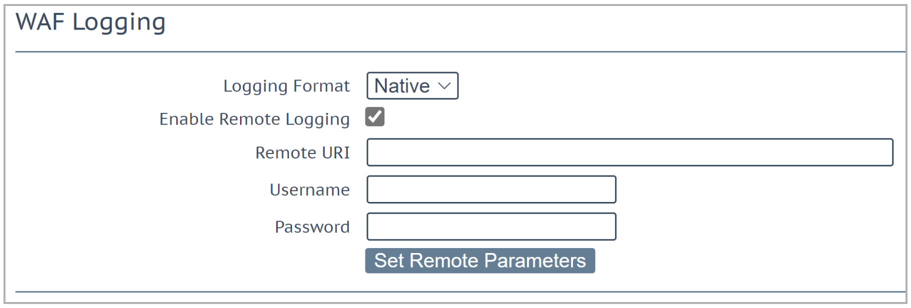
> A WAF configuration can only be restored onto a LoadMaster with a WAF license.

2.7 WAF Logging, Statistics and Status Options

This section describes the WAF Logging, Statistics and Status options available in the LoadMaster UI.

2.7.1 Export Logs in the Web Application Firewall menu

You can get to this screen by selecting **Web Application Firewall > Export Logs** in the main menu of the LoadMaster UI.



WAF Logging

Logging Format: Native

Enable Remote Logging ☑

Remote URI

Username

Password

Logging Format

Select either Native or JSON depending on what format you want the audit logs to appear.

Enable Remote Logging

This check box enables you to enable or disable remote logging for WAF.

Remote URI

Specify the Uniform Resource Identifier (URI) for the remote logging server.

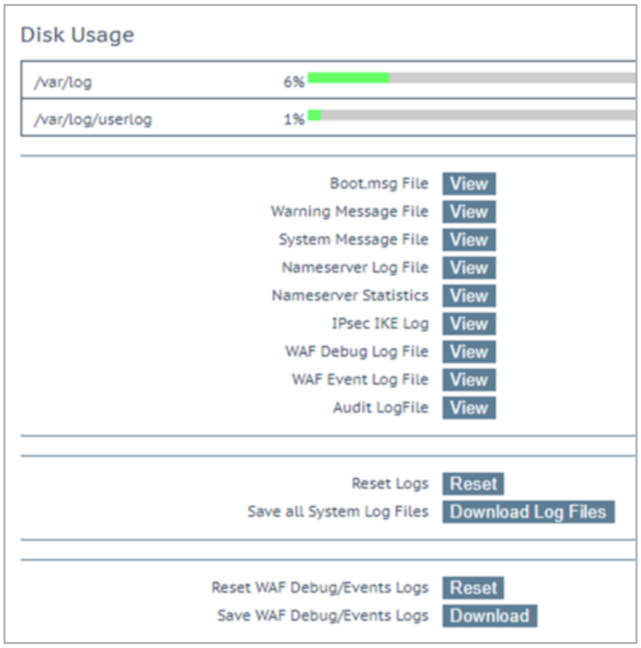
Username

Specify the username for the remote logging server.

Password

Specify the password for the remote logging server.

2.7.2 WAF Event Log



Disk Usage

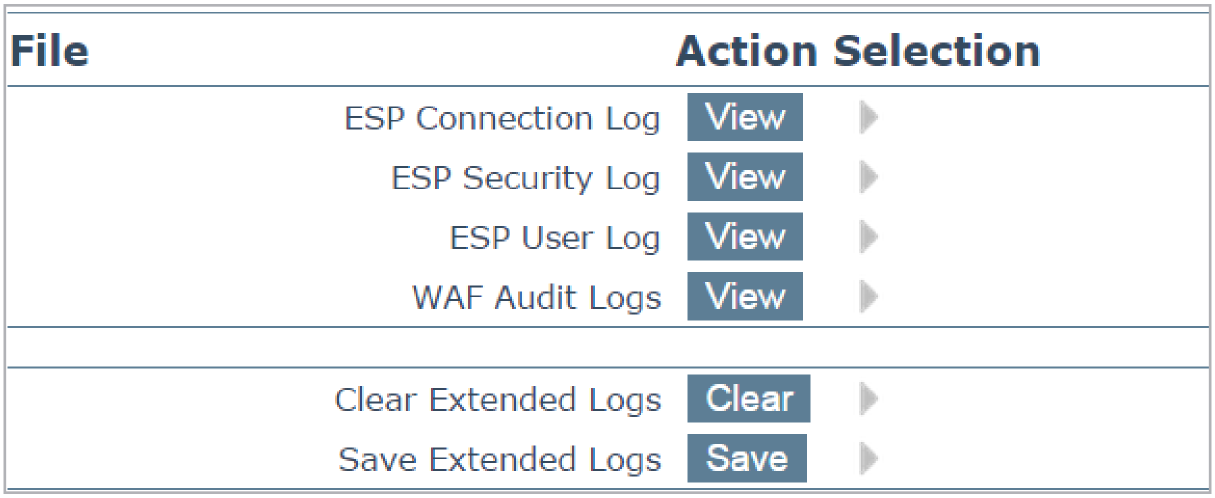
/var/log	6%
/var/log/userlog	1%

Boot.msg File	View
Warning Message File	View
System Message File	View
Nameserver Log File	View
Nameserver Statistics	View
IPsec IKE Log	View
WAF Debug Log File	View
WAF Event Log File	View
Audit LogFile	View
Reset Logs	Reset
Save all System Log Files	Download Log Files
Reset WAF Debug/Events Logs	Reset
Save WAF Debug/Events Logs	Download

You can view the WAF Event Log by going to **System Configuration > Logging Options > System Log Files** and clicking the relevant **View** button. This log file contains all WAF alerts and automatically updates to show new events.

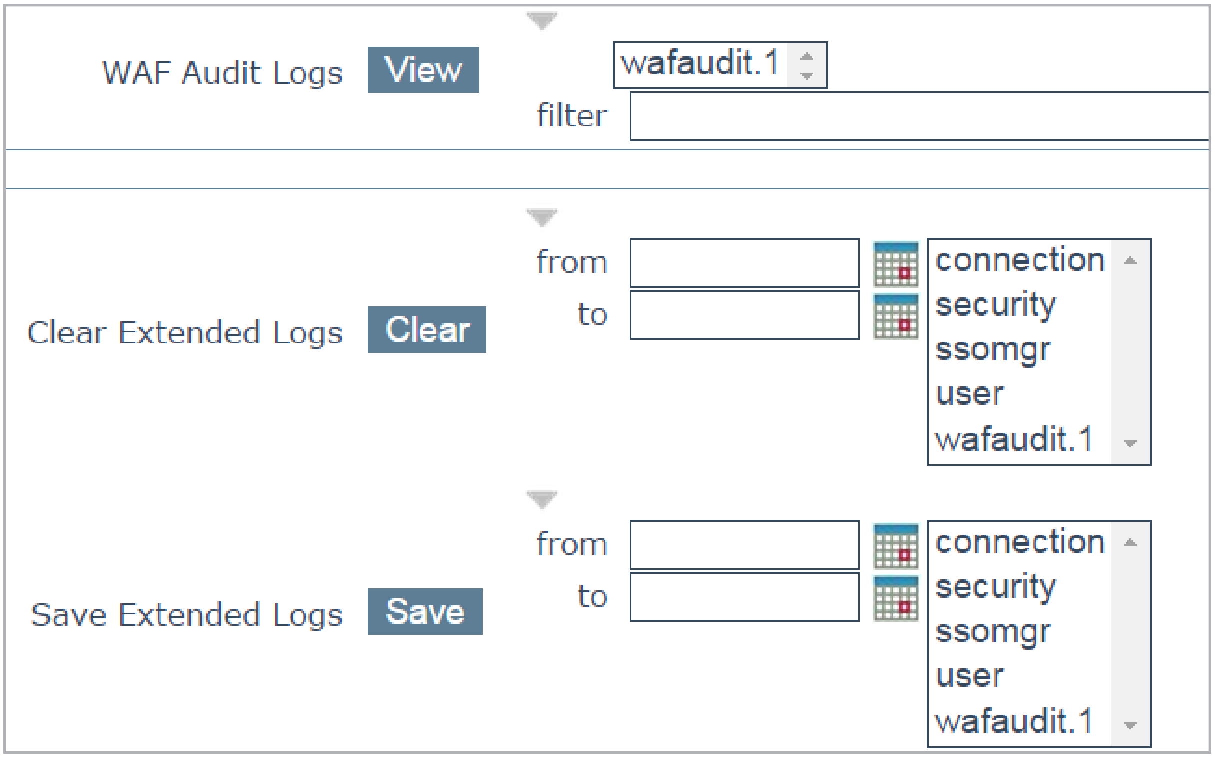
You can also reset and/or download the WAF debug/event logs by clicking the relevant buttons.

2.7.3 WAF Options in the Extended Log Files Screen



File	Action Selection
ESP Connection Log	View
ESP Security Log	View
ESP User Log	View
WAF Audit Logs	View
Clear Extended Logs	Clear
Save Extended Logs	Save

The **Extended Log Files** screen provides options for logs relating to the ESP and WAF features. These logs are persistent and will be available after a LoadMaster reboot. To view all of the options click the ▸ icons.



> In addition to WAF logs, ESP logs are also available on this screen. For more information, refer to the **Edge Security Pack (ESP), Feature Description**.

WAF Audit Logs: recording WAF logs based on what has been selected for the **Audit mode** drop-down list (either **Audit Relevant** or **Audit All**) in the **WAF Options** section of the Virtual Service modify screen.

To view the logs, select the appropriate log file and click the relevant **View** button.

The number listed in each log entry corresponds to the ID of the Virtual Service. To get the Virtual Service ID, first ensure that the API interface is enabled (**Certificates & Security > Remote Access > Enable API Interface**). Then, in a web browser address bar, enter **https://<LoadMasterIPAddress>/access/listvs**. Check the **index** of the Virtual Service. This is the number that corresponds to the number on the audit log entry.

One or more archived log files can be viewed by selecting the relevant file(s) from the list of file names and clicking the **View** button. You can filter the log files by entering a word(s) or regular expression in the **filter** field and clicking the **View** field.

Clear Extended Logs

All extended logs can be deleted by clicking the **Clear** button.

Specific log files can be deleted by filtering on a specific date range, selecting one or more individual log files in the log file list or selecting a specific log type (for example, connection, security or user) in the log file list and clicking the **Clear** button. Click **OK** on any warning messages.

Save Extended Logs

All extended logs can be saved to a file by clicking the **Save** button.

Specific log files can be saved by filtering on a specific date range, selecting one or more individual log files in the log file list or selecting a specific log type (for example connection, security or user) in the log file list and clicking the **Save** button.

2.7.4 Enable WAF Debug Logging

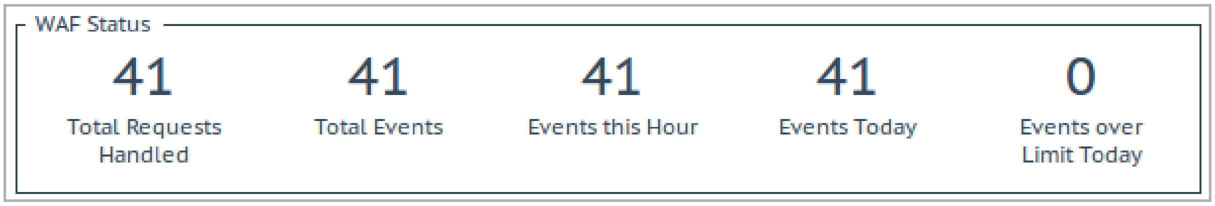
WAF debug traces can be enabled by clicking the **Enable Logging** button at **System Configuration > Logging Options > System Log Files**.

> This generates a lot of log traffic. It also slows down WAF processing. Only enable this option when requested to do so by Kemp Technical Support. Kemp does not recommend enabling this option in a production environment.

The WAF debug logs are never closed, and they are rotated if they get too large. WAF (in general) needs to be disabled and re-enabled (by clearing and re-selecting the **Enabled** check box) in all WAF-enabled Virtual Service settings to re-enable the debug logs. Alternatively, perform an update (in the **Web Application Firewall > Custom Rules** screen), with daily updates that are relevant for the Virtual Service(s).

2.7.5 WAF Statistics

2.7.5.1 Home Page



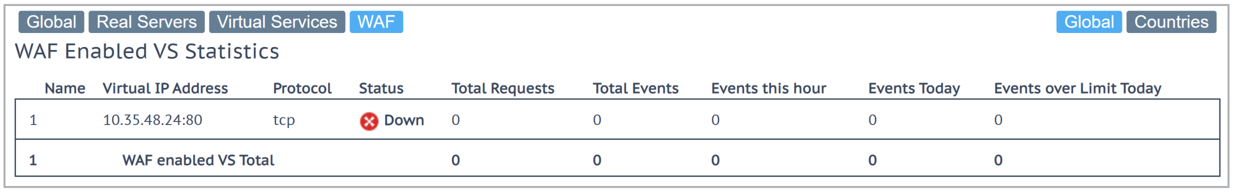
WAF Status

Total Requests Handled	Total Events	Events this Hour	Events Today	Events over Limit Today
41	41	41	41	0

The **WAF Status** section is displayed on the UI home page if at least one Virtual Service has WAF enabled. The values shown here are as follows:

- The total number of requests handled by the WAF shows all requests, whether they were blocked or not. Two requests are recorded for each connection – one incoming and one outgoing request.
- The total number of events handled by the WAF, therefore requests that were blocked.
- The number of events that have happened in the current hour since xx.00.00.
- The number of events that have happened since 00.00 am local time.
- The number of times the event counter has gone over the configured warning threshold today. For example, if the threshold is set to 10 and there have been 20 events, this counter will be set to 2. The warning threshold is set on a per-Virtual Service basis by filling out the **Hourly Alert Notification Threshold** field in either **WAF Options (Legacy) or WAF sections** in the Virtual Service modify screen.

2.7.5.2 Statistics Page



WAF Enabled VS Statistics

	Name	Virtual IP Address	Protocol	Status	Total Requests	Total Events	Events this hour	Events Today	Events over Limit Today
1		10.35.48.24:80	tcp	✖ Down	0	0	0	0	0
1	WAF enabled VS Total				0	0	0	0	0

To get to the WAF statistics page in the LoadMaster UI, go to **Statistics > Real Time Statistics > WAF > Global**. These statistics refresh every 5 to 6 seconds. The following items are displayed on this screen:

Count: The left-most column displays the total number of WAF-enabled Virtual Services.

Name: The name of the WAF-enabled Virtual Service.

Virtual IP Address: The IP address and port of the Virtual Service.

Protocol: The protocol of the Virtual Service (tcp or udp).

Status: Displays the status of the Virtual Service. For information on each of the possible statuses, refer to the **Web User Interface (WUI), Configuration Guide**.

Total Requests: The total number of requests handled by the WAF and shows all requests, whether they were blocked or not. Two requests are recorded for each connection – one incoming and one outgoing request.

Total Events: The total number of events handled by the WAF (therefore, requests that were blocked).

Events this hour: The number of events that have happened in the current hour since xx.00.00.

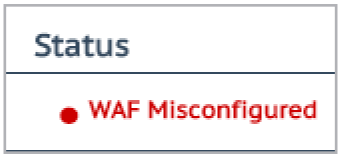
Events Today: The number of events that have happened since 00.00 am local time.

Events over Limit Today: The number of times the event counter has gone over the configured warning threshold today. For example, if the threshold is set to 10 and there have been 20 events, this counter will be set to 2. The warning threshold is set on a per-Virtual Service basis by filling out the **Hourly Alert Notification Threshold** field in either **WAF Options (Legacy) or WAF sections** in the Virtual Service modify screen.

Countries: Click the **Countries** button in the top right of the page to display the screen that contains a list of top 10 blocked countries.

These WAF statistics can also be seen in the Virtual Service statistics screen (go to **Statistics > Real Time Statistics > Virtual Services** and then click the **Virtual IP Address** link).

2.7.6 WAF Misconfigured Virtual Service Status



Status
● WAF Misconfigured

On the **View/Modify Services** screen in the LoadMaster UI, the **Status** of each Virtual Service is displayed. If the WAF for a particular Virtual Service is misconfigured (for example, if there is an issue with a rule file), the status changes to **WAF Misconfigured** and turns to red.

> If the Virtual Service is in a **WAF Misconfigured** state, all traffic stops flowing. WAF can be disabled for that Virtual Service to stop the traffic being blocked, if required, while troubleshooting the problem.

3 Troubleshooting

Refer to the sections below for some information relating to WAF troubleshooting.

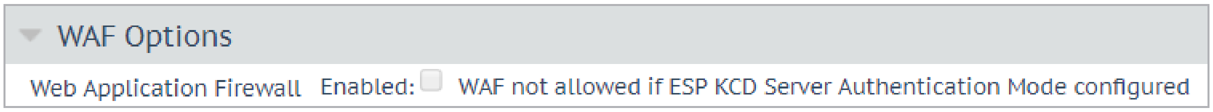
3.1 WAF Logging

All events are logged but there may be a delay in them being available for Administrator viewing. For further information on the WAF logging options, refer to the **WAF Event Log** and **Enable WAF Debug Logging** sections.

3.2 WAF Compatibility with Kerberos Constrained Delegation (KCD)

As of the 7.2.40 LoadMaster firmware version, you cannot enable both WAF and KCD at the same Virtual Service level. For example:

- If WAF is enabled in the parent Virtual Service, you cannot enable KCD as the **Server Authentication Mode** in the parent Virtual Service



WAF Options

Web Application Firewall Enabled: □ WAF not allowed if ESP KCD Server Authentication Mode configured

- If KCD is enabled in the parent Virtual Service, you cannot enable WAF

However, you can enable ESP/KCD in the SubVS and then enable WAF in the parent Virtual Service.

If you had WAF and KCD enabled at the same level before upgrading to 7.2.40 and you upgrade the firmware to 7.2.40 or above, the configuration will not be changed. File attachments in SharePoint will not work. To resolve this, enable WAF on the parent Virtual Service and ESP/KCD on the SubVS.

The following combination is not supported: WAF with ESP Client Certificate authentication and KCD.

3.3 Unable to Download/Update Daily Updates

Kemp recommends adding the Kemp Licensing Server URLs as allowed URLs on your firewall to ensure all licensing features work, including the downloading and updating of WAF daily updates. The URLs to allow vary depending on your LoadMaster firmware version:

- LoadMaster firmware version 7.2.53 or above (or 7.2.48.3 Long Term Support (LTS) and above): **licensing.kemp.ax**
- LoadMaster firmware versions below 7.2.53 (or below 7.2.48.3 LTS): **alsi.kemptechnologies.com** and **alsi2.kemptechnologies.com**

Appendix A: Legacy Rules

The following sections provide more information about how to configure the legacy WAF rules.

> The Legacy WAF rules are being retired on 29th June 2021, and no further updates will be available. It is recommended to migrate your configuration to the new WAF services.

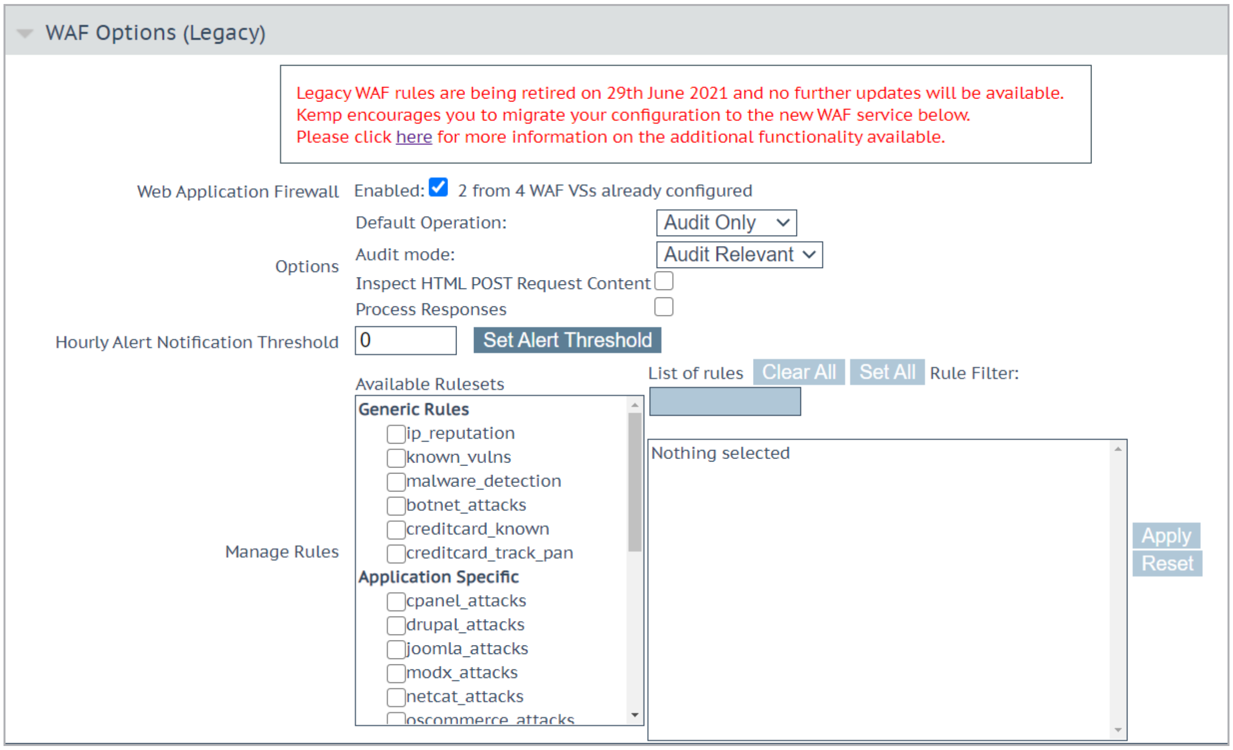
Configure WAF Options (Legacy) for a Virtual Service

WAF settings can be configured for each Virtual Service. Follow the steps below to configure the WAF options (Legacy) in a Virtual Service. For more information on each of the fields, refer to the **<b>WAF UI Options</b>** section.

1. In the main menu of the LoadMaster UI, select **Virtual Services > View/Modify Services**.

2. Click **Modify** on the relevant Virtual Service.

3. Expand the **WAF Options (Legacy)** section.



WAF Options (Legacy)

Legacy WAF rules are being retired on 29th June 2021 and no further updates will be available.
Kemp encourages you to migrate your configuration to the new WAF service below.
Please click here for more information on the additional functionality available.

Web Application Firewall Enabled: ☑ 2 from 4 WAF VSs already configured

Options
Default Operation: Audit Only
Audit mode: Audit Relevant
Inspect HTML POST Request Content ☐
Process Responses ☐

Hourly Alert Notification Threshold 0

Manage Rules

Available Rulesets

Generic Rules
☐ ip_reputation
☐ known_vulns
☐ malware_detection
☐ botnet_attacks
☐ creditcard_known
☐ creditcard_track_pan

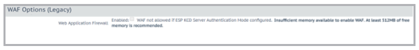
Application Specific
☐ cpanel_attacks
☐ drupal_attacks
☐ joomla_attacks
☐ modx_attacks
☐ netcat_attacks
☐ oscommerce_attacks

List of rules — Nothing selected

4. By default, WAF is disabled. To enable WAF, select **Enabled**.

   When WAF is enabled for a Virtual Service, the section heading in the Virtual Service options changes from **WAF Options (Legacy)** to **WAF Options (Legacy - Enabled)**

   The maximum number of WAF-enabled Virtual Services is the total (unused or available) RAM (in MB)/512 MB. For example: 8 GB/512 MB = 16 WAF-enabled Virtual Services. When the maximum is reached, no additional Virtual Services can be enabled with WAF.



WAF Options (Legacy)

Web Application Firewall Enabled: □ WAF not allowed if ESP KCD Server Authentication Mode configured. **Insufficient memory available to enable WAF. At least 512MB of free memory is recommended.**

   A message displays if there is insufficient memory available to enable WAF.

   A message is displayed next to the **Enabled** check box showing how many WAF-enabled Virtual Services exist and the maximum number of WAF-enabled Virtual Services that can exist. If the maximum number of WAF-enabled Virtual Services is reached, the **Enabled** check box is greyed out.

5. Specify the **Default Operation** type.

   The **Default Operation** is what occurs if no action is specified in the relevant rule.

   Audit Only: This is an audit-only mode – logs are created, but requests and responses are not blocked.

   Block Mode: Either requests or responses are blocked based on the assigned rules.

6. Specify the **Audit mode**.

   There are three audit modes:
   - **No Audit:** No data is logged.
   - **Audit Relevant:** Logs data that is of a warning level and higher. This is the default option for this setting.
   - **Audit All:** Logs all data through the Virtual Service.

> Selecting the **Audit All** option produces a large amount of log data. Kemp does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

7. Specify whether or not to **Inspect HTML POST Request Content**.

The **Inspect HTML POST Request Content** option is disabled by default. If you enable this option, three more check boxes become available that allow you to enablethe processing of JavaScript Object Notation (JSON), XML requests, and other content types.

8. Enable **Process Responses** to verify response data sent from the Real Servers. .

The processing of response data can be CPU and memory intensive.

9. Specify the **Hourly Alert Notification Threshold** and click **Set Alert Threshold**.

This is the number of incidents per hour before sending an alert. Setting this to **0** disables alerts.

10. Assign rulesets by selecting them in the **Available Rulesets** section.

11. Individual rules can be enabled/disabled per ruleset by selecting/clearing them in the box on the right.

Rules can be filtered by entering a filter term in the **Rule Filter** text box.
Clicking **Clear All** disables all rules for the selected ruleset.
Clicking **Set All** enables all rules for the selected ruleset.
Clicking the **Reset** button disables any rule sets and rules selected since the last time you clicked **Apply**.

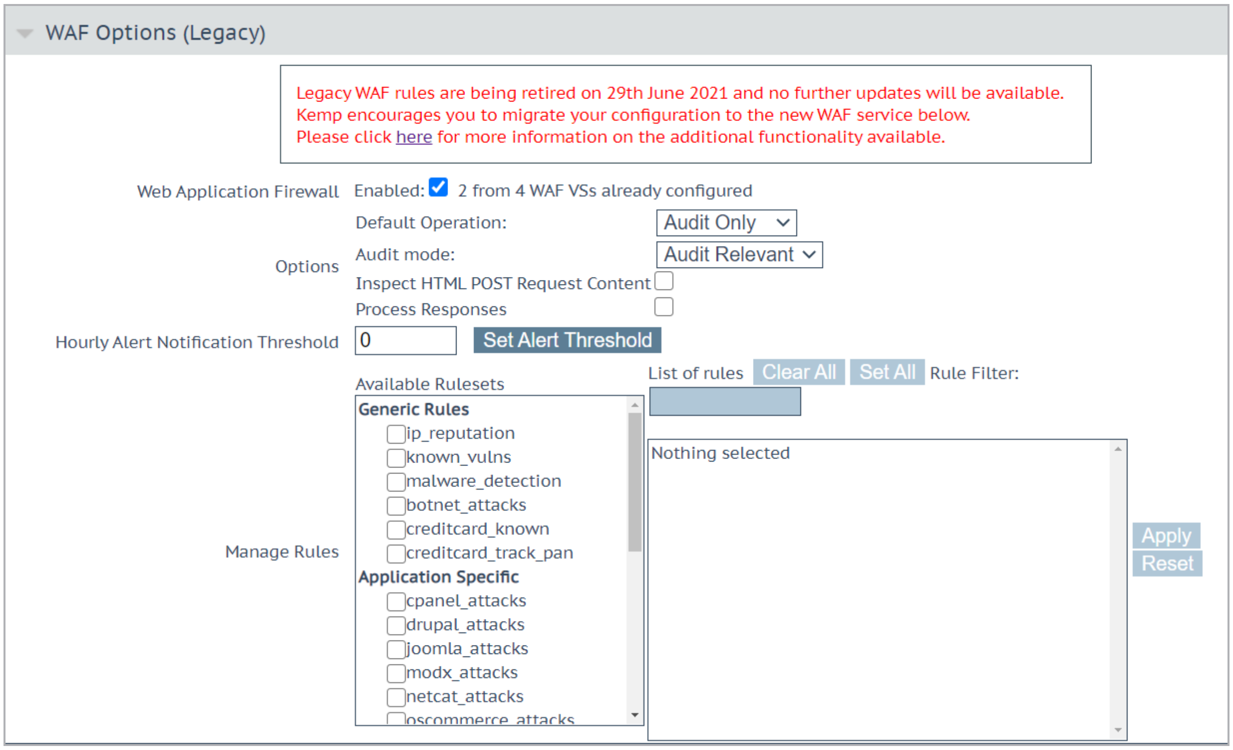
12. When finished enabling/disabling the relevant rulesets and rules, click **Apply**.

Application-specific and application-generic rules cannot both be assigned to the same Virtual Service. If you try to do this, an error message (**Cannot assign Application Specific and Application Generic rules simultaneously**) appears to inform you that this is not possible.

WAF Options (Legacy) in the Virtual Service Modify Screen

You can get to the Virtual Service WAF Options by selecting **Virtual Services > View/Modify Services** in the main menu, clicking **Modify** on the relevant Virtual Service and expanding the **WAF Options (Legacy)** section.

By default, WAF is disabled. To enable WAF on this Virtual Service, select the **Enabled** check box. This must be enabled to configure any further options.



WAF Options (Legacy)

Legacy WAF rules are being retired on 29th June 2021 and no further updates will be available.
Kemp encourages you to migrate your configuration to the new WAF service below.
Please click here for more information on the additional functionality available.

Web Application Firewall Enabled: ☑ 2 from 4 WAF VSs already configured

Options
Default Operation: Audit Only
Audit mode: Audit Relevant
Inspect HTML POST Request Content □
Process Responses □

Hourly Alert Notification Threshold 0

Manage Rules
Available Rulesets
Generic Rules
□ ip_reputation
□ known_vulns
□ malware_detection
□ botnet_attacks
□ creditcard_known
□ creditcard_track_pan
Application Specific
□ cpanel_attacks
□ drupal_attacks
□ joomla_attacks
□ modx_attacks
□ netcat_attacks
□ oscommerce_attacks

List of rules Rule Filter:
Nothing selected

Default Operation

Specify the Default Operation type:

- **Audit Only:** This is an audit-only mode – logs are created, but requests and responses are not blocked. It is recommended when first using WAF to enable **Audit Only** mode for a while. During this time you should analyze the logs and adjust the rules and settings as needed before enabling **Block Mode** . This ensures that no legitimate traffic is blocked.
- **Block Mode:** Either requests or responses are blocked based on the assigned rules.

Audit mode

Audit logs are produced according to the specifications on the following website: https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-2-Data-Formats

Select what logs to record:

- **No Audit:** No data is logged.
- **Audit Relevant:** Logs data which is of a warning level and higher. This is the default option for this setting.
- **Audit All:** Logs all data through the Virtual Service.

Selecting the **Audit All** option produces a large amount of log data. Kemp does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

Inspect HTML POST Request Content

Enable this option to also process the data supplied in POST requests.

The **Inspect HTML POST Request Content** option is disabled by default. If you enable this option, three more check boxes become available that allow you to enable the processing of JavaScript Object Notation (JSON), XML requests, and other content types.

Enable verification of JavaScript Object Notation (JSON) POST requests.

Enable XML Parser

Enable verification of Extensible Markup Language (XML) POST requests.

Enable Other Content Types

Enable verification of POST content types (other than XML/JSON).

Enabling the inspection of any other content types may increase system resource utilization (CPU and memory). A specific list of content types should be considered.

When the **Enable Other Content Types** option is enabled, there is a text box to enter a comma-separated list of POST content types allowed for WAF analysis. By default, all types (other than XML/JSON) are enabled.

WAF does not block attack requests if the POST request does not contain the 'content-type' header, even if **Inspect HTML POST Request Content**, **Enable JSON Parser**, **Enable XML Parser**, and Enable **Other Content Types** check boxes are all enabled. This is a WAF rule issue and can be solved by having a rule to check if there is no 'content-type' present in the request header and forcing the URL-encoded parser in the WAF rules.

Process Responses

Enable this option to verify response data sent from the Real Servers.

> This can be CPU and memory-intensive, so only enable this if necessary.

> If a Real Server is gzip encoding, WAF will not check that traffic, even if **Process Responses** is enabled.

Hourly Alert Notification Threshold

This is the threshold of incidents per hour before sending an alert email. Setting this to **0** disables alerting.

Rules

This is where you can assign/un-assign generic, application-specific, application-generic, and custom rules to and from the Virtual Service.

> You cannot assign application-specific and application-generic rules to the same Virtual Service.

Individual rules within each ruleset can be enabled/disabled as required. To enable a ruleset, select the relevant check box. If you have not enabled/disabled rules in that ruleset previously, all rules are enabled by default in the right box. If you have previously enabled/disabled rules in that ruleset, within that Virtual Service – the rules retain their previous settings.

You can enable/disable individual rules as needed by selecting the relevant ruleset on the left and selecting/clearing the rules on the right.

> Some rules or rule sets may have dependencies on other rules. There is no dependency check in the LoadMaster when rules are disabled - before disabling any rule, be aware of any rule chains or dependencies.

When finished making changes, click **Apply**.

Clicking the **Clear All** button disables all rules for the selected ruleset.

Clicking the **Set All** button enables all rules for the selected ruleset.

Text can be entered in the **Rule Filter** text box to filter the rules to only show rules that contain the filter text.

Clicking **Reset** disables all rulesets and rules.

> Only assign the rules that are required. All assigned rules will be checked against, so a large number of assigned rules can lead to high CPU usage.

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation

Edge Security Pack (ESP), Feature Description

Kemp LoadMaster, Product Overview

Web User Interface (WUI), Configuration Guide

Last Updated Date

This document was last updated on 27 April 2021.